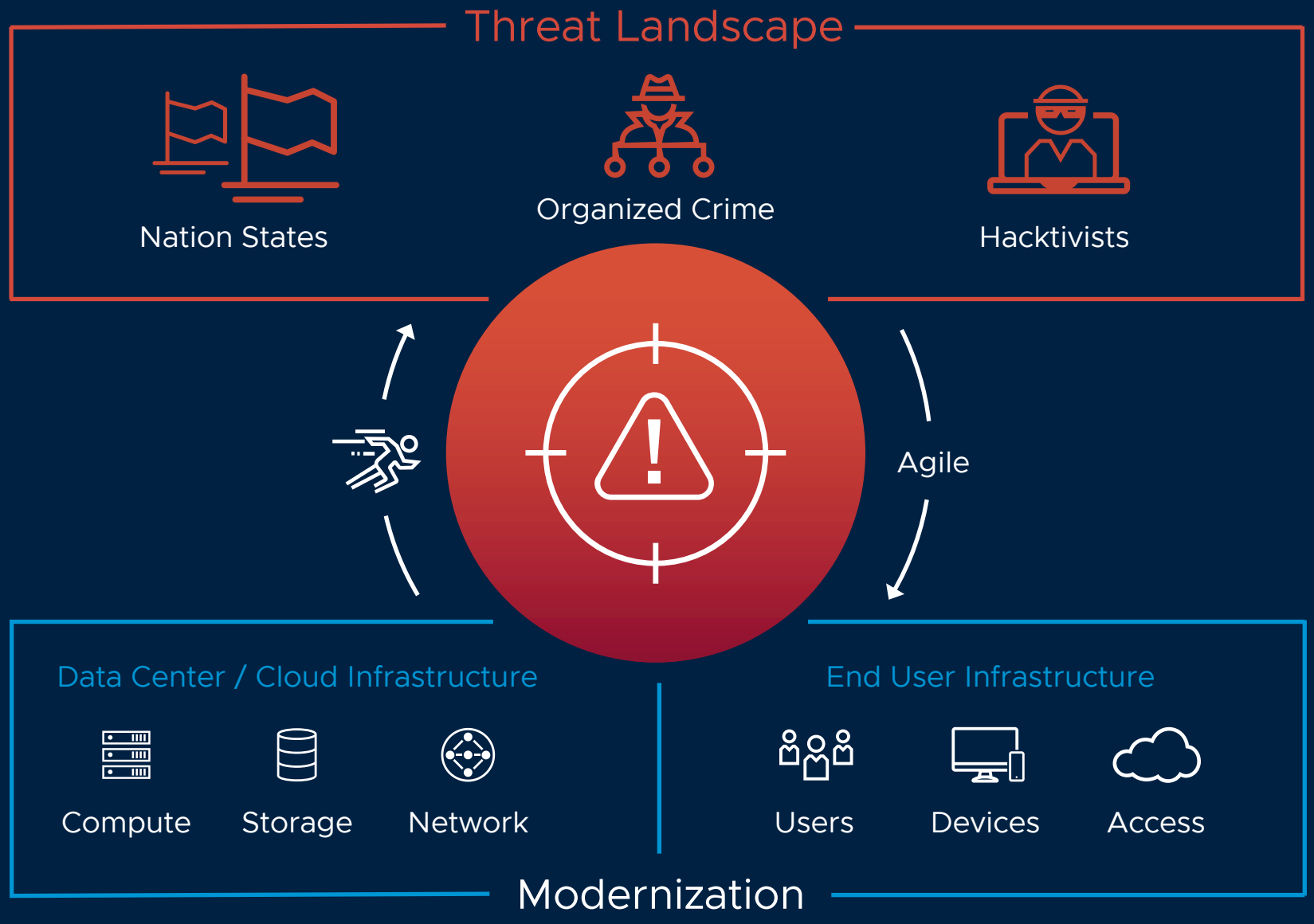
Moving from an Infrastructure to an Application Security Focus

Scottie Ray—Architect
VMware Network & Security Virtualization
sray@vmware.com
@H2Only

vmware

The Taxonomy is Difficult Enough

SDDC	FaaS	Cyber	SaaS	DevOps
Multi-factor	Policy Framework	IoT	Cloud	Security
Agility	Context	OpsSec	Resiliency	Containers
IaaS	Microsegmentation	PaaS	CI/CD	MDM
Abstraction	Hybridity	Threat Landscape	Compliance	Service Mesh



Forecasted Growth in Overall IT Spend

4.5%

$3.7 Trillion in 2018

Gartner Press Release, Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018, January 16, 2018

Growth in Security Spend

10.2%
(since 2017)

$91.4 Billion in 2018

Source: IDC, Worldwide Semiannual Security Spending Guide, #US42570018, March 2018

Increase in Security Losses

26%
(since 2014)

$600 Billion in 2017

Source: Center for Strategic and Int'l Studies, Economic Impact of Cybercrime, February, 2018

The Response by Industry

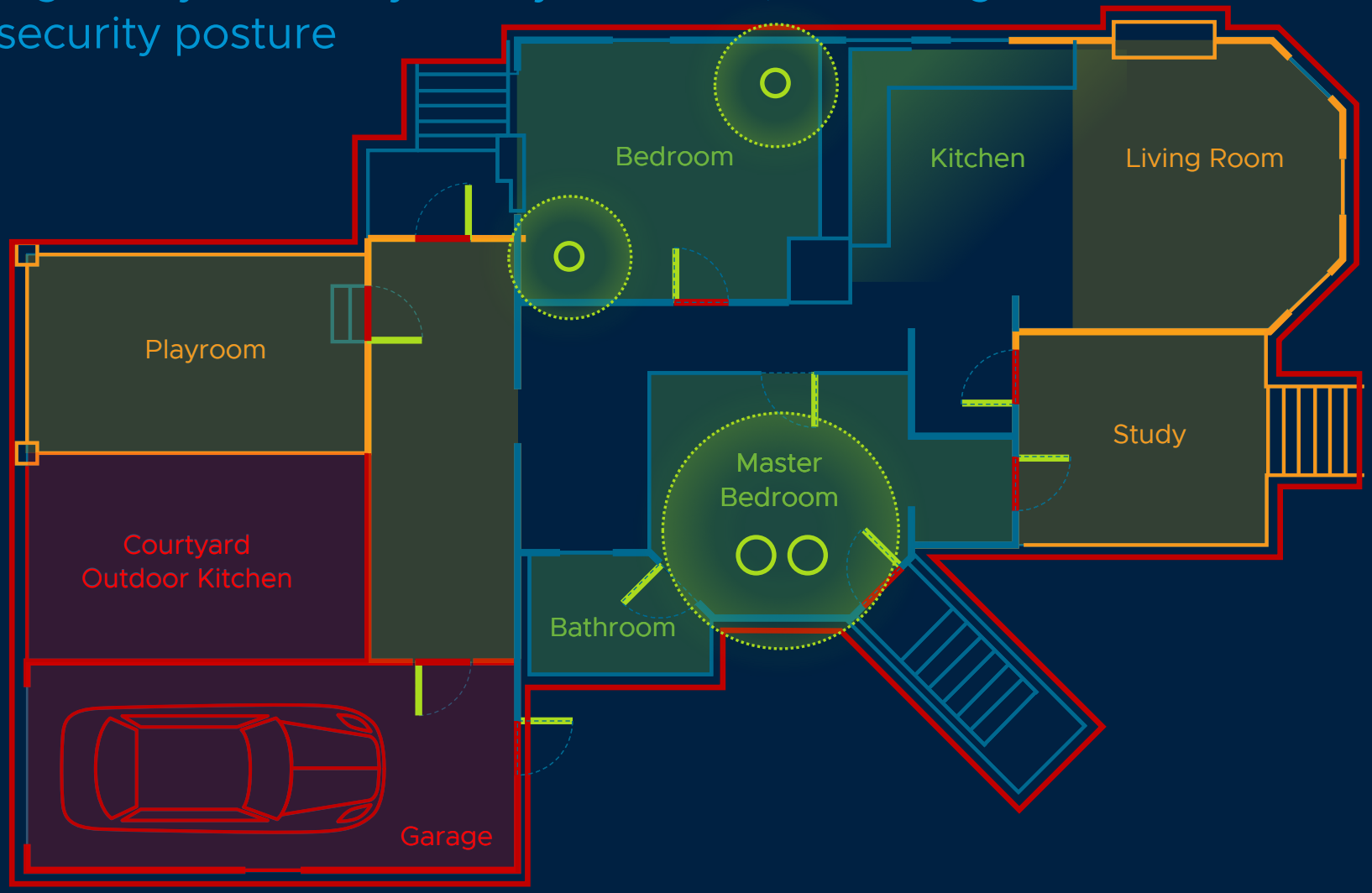
One Key to Security Focused Agility is Contextual Understanding

The Contextual Advantage

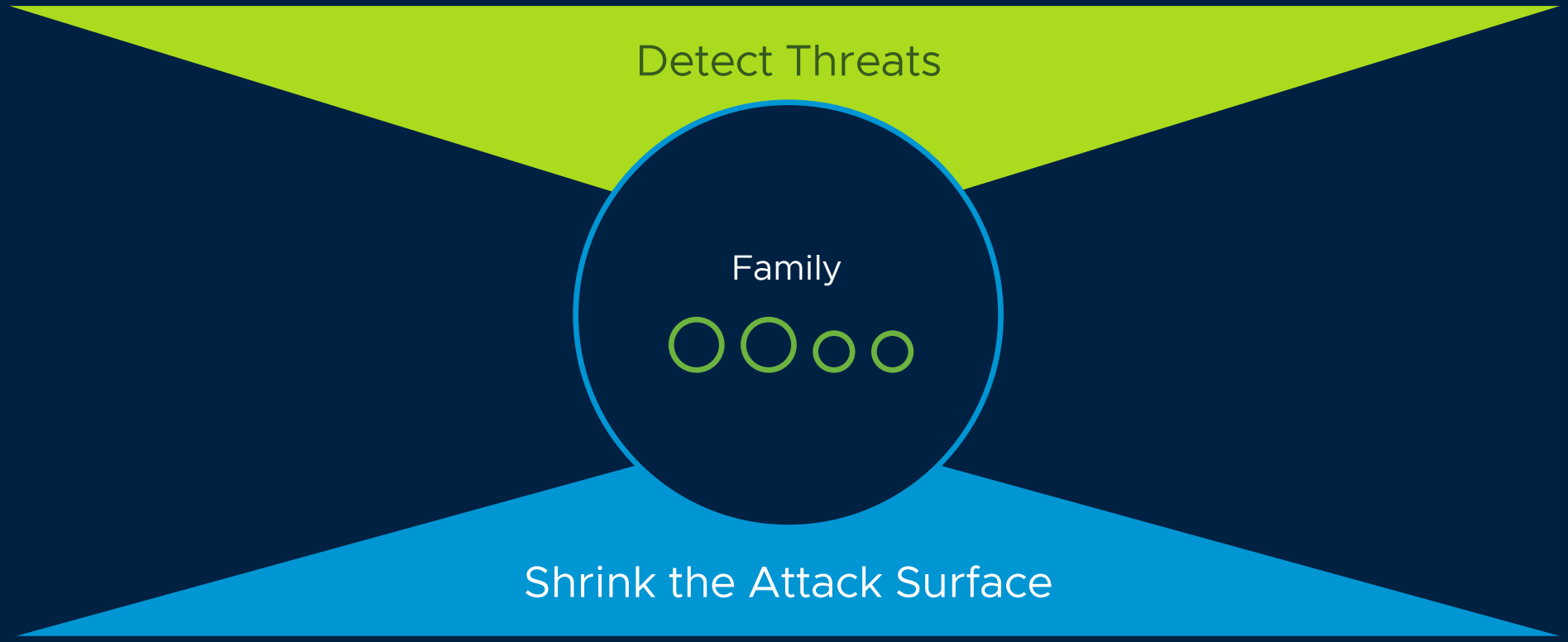
An Analogy of a System….

Understanding how your family uses your home, and using that context to shrink your security posture

Family



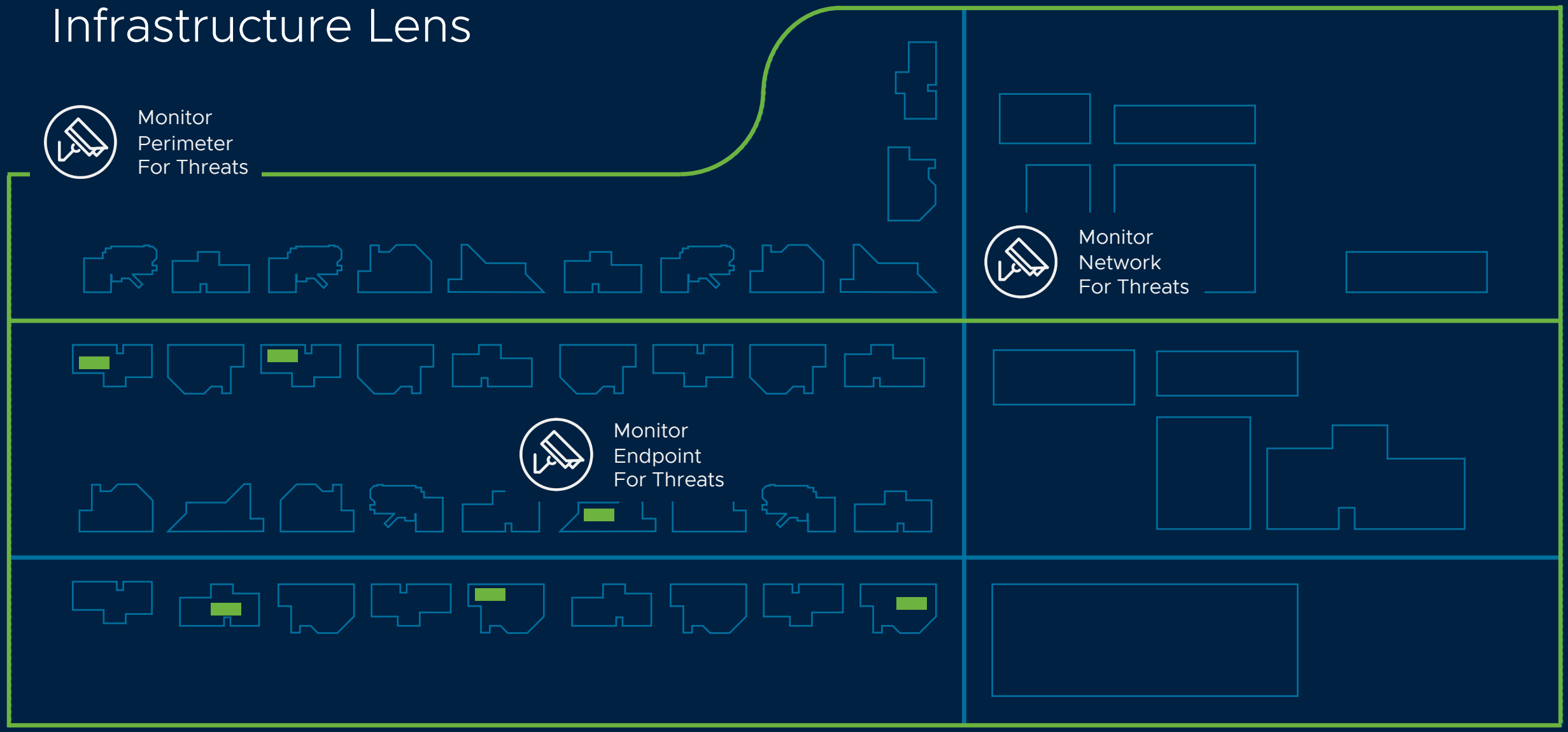
Context Creates Advantage



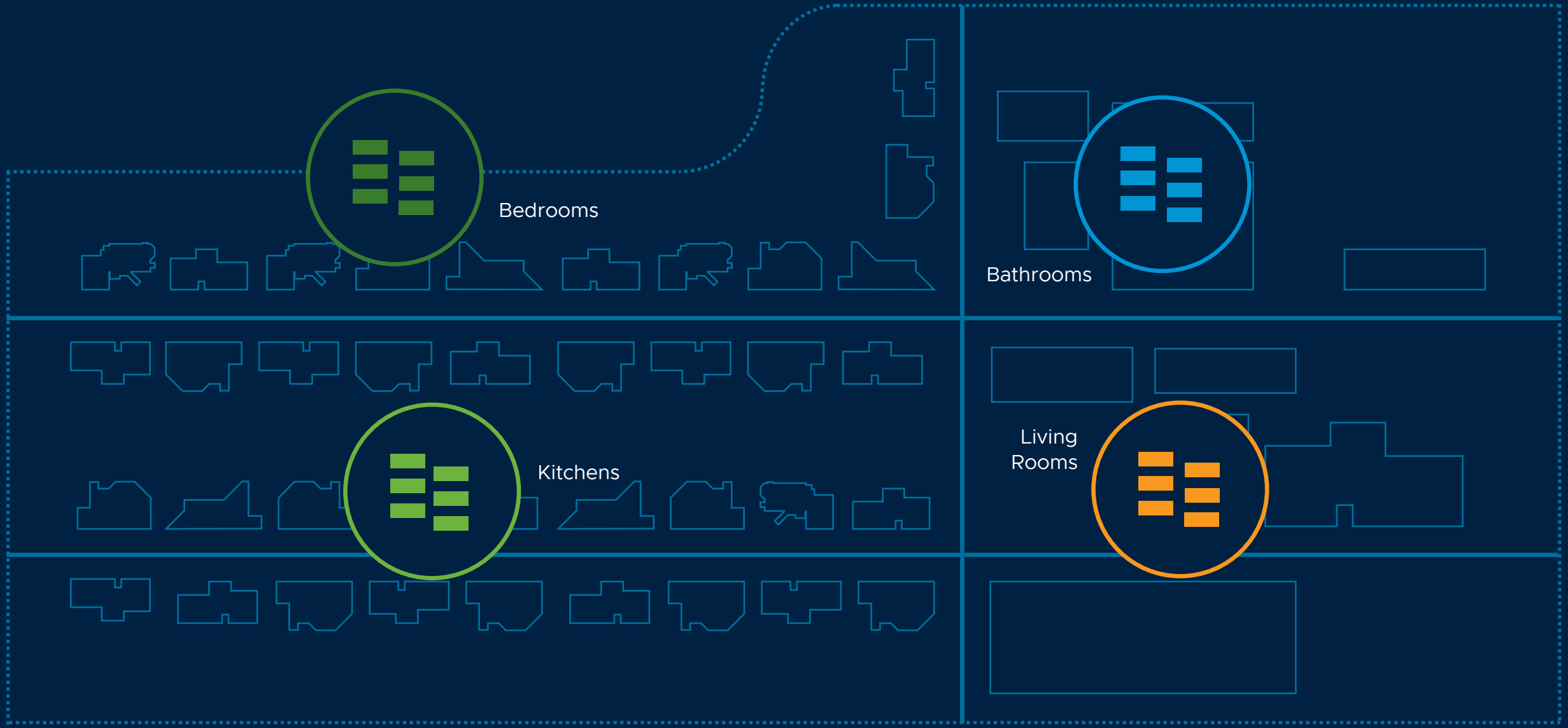
The Problem of Context within Security Architectures

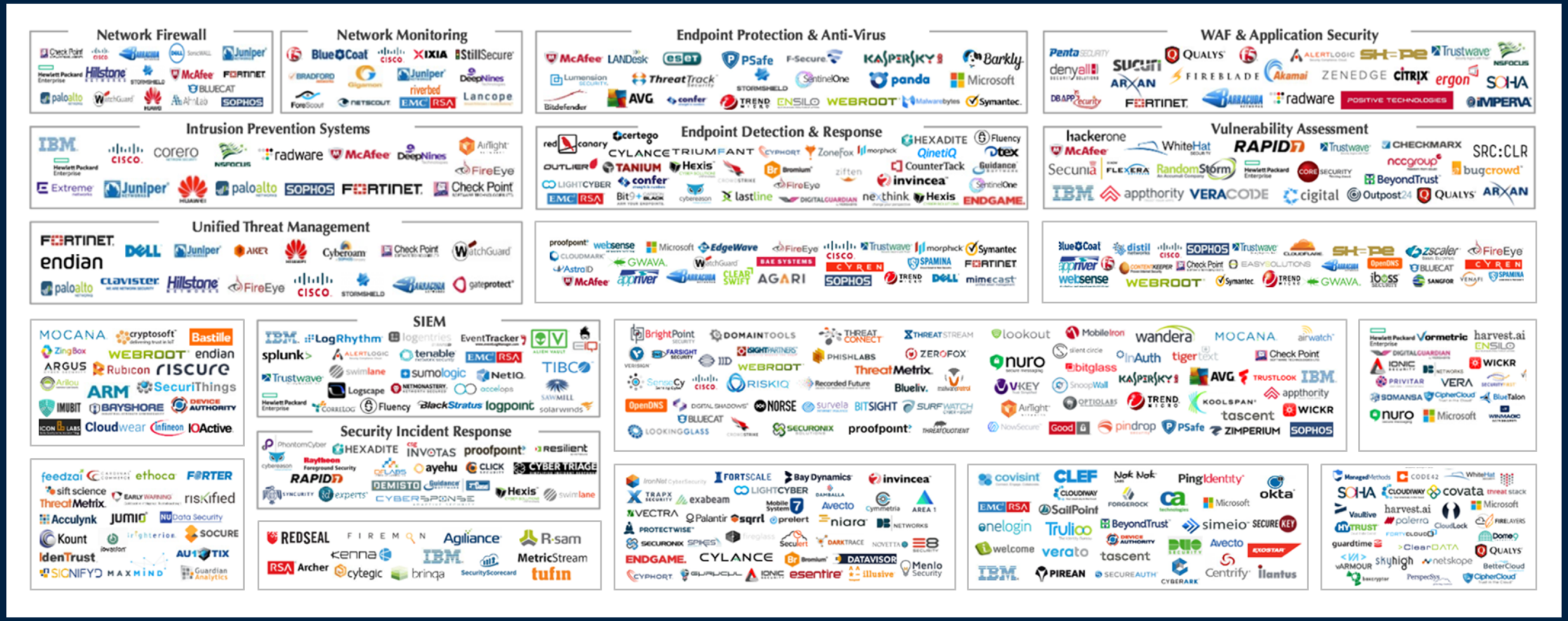
We Keep All the Lights On, and All the Rooms Open

We See Security Through an Infrastructure Lens



If We Compartmentalize at All, it's Aligned to an Infrastructure Lens

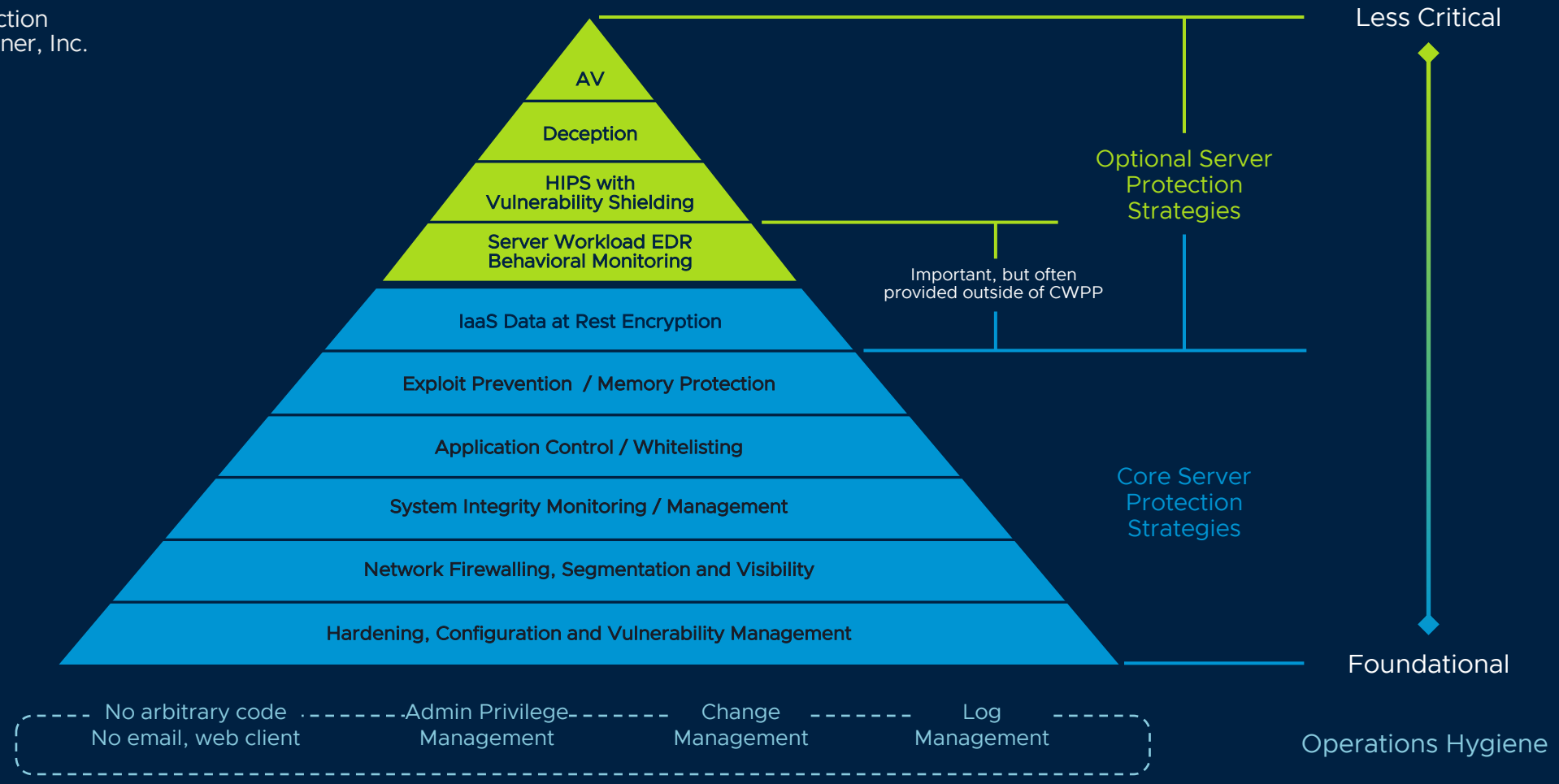



Network Firewall
Network Monitoring
Endpoint Protection & Anti-Virus
WAF & Application Security
Intrusion Prevention Systems
Endpoint Detection & Response
Vulnerability Assessment
Unified Threat Management
SIEM
Security Incident Response

We Should Focus More on Core Protection Strategies

Gartner Market Guide for Cloud Workload Protection Framework

Figure 1. Cloud Workload Protection Controls Hierarchy, © 2018 Gartner, Inc.



Source: Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald, March 26th 2018. *Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document.*

Cyber Threats
Residual Risk

Micro-Segmentation

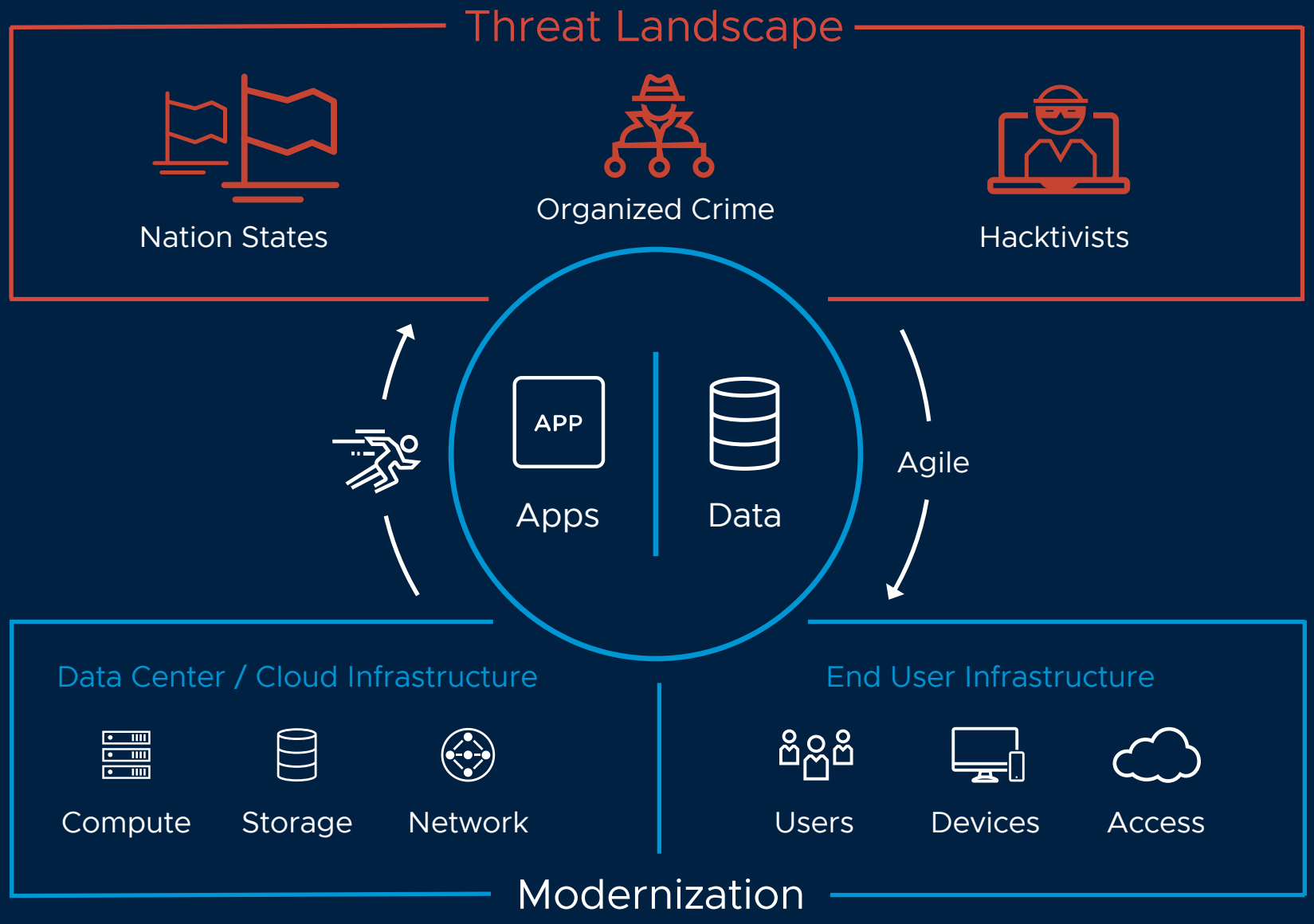
Least Privilege

Encryption

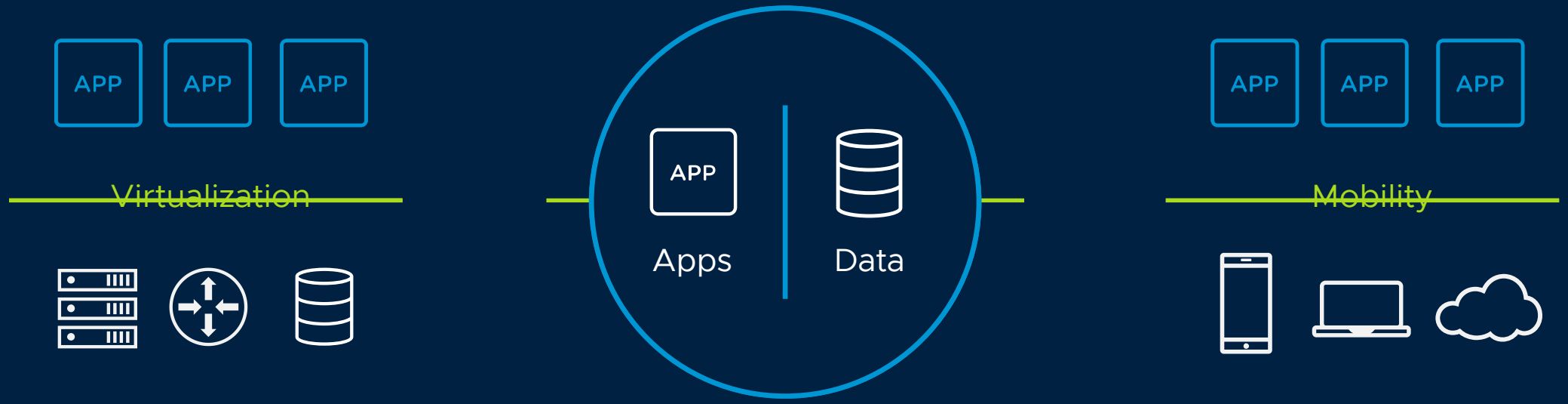
Multi-Factor Authentication

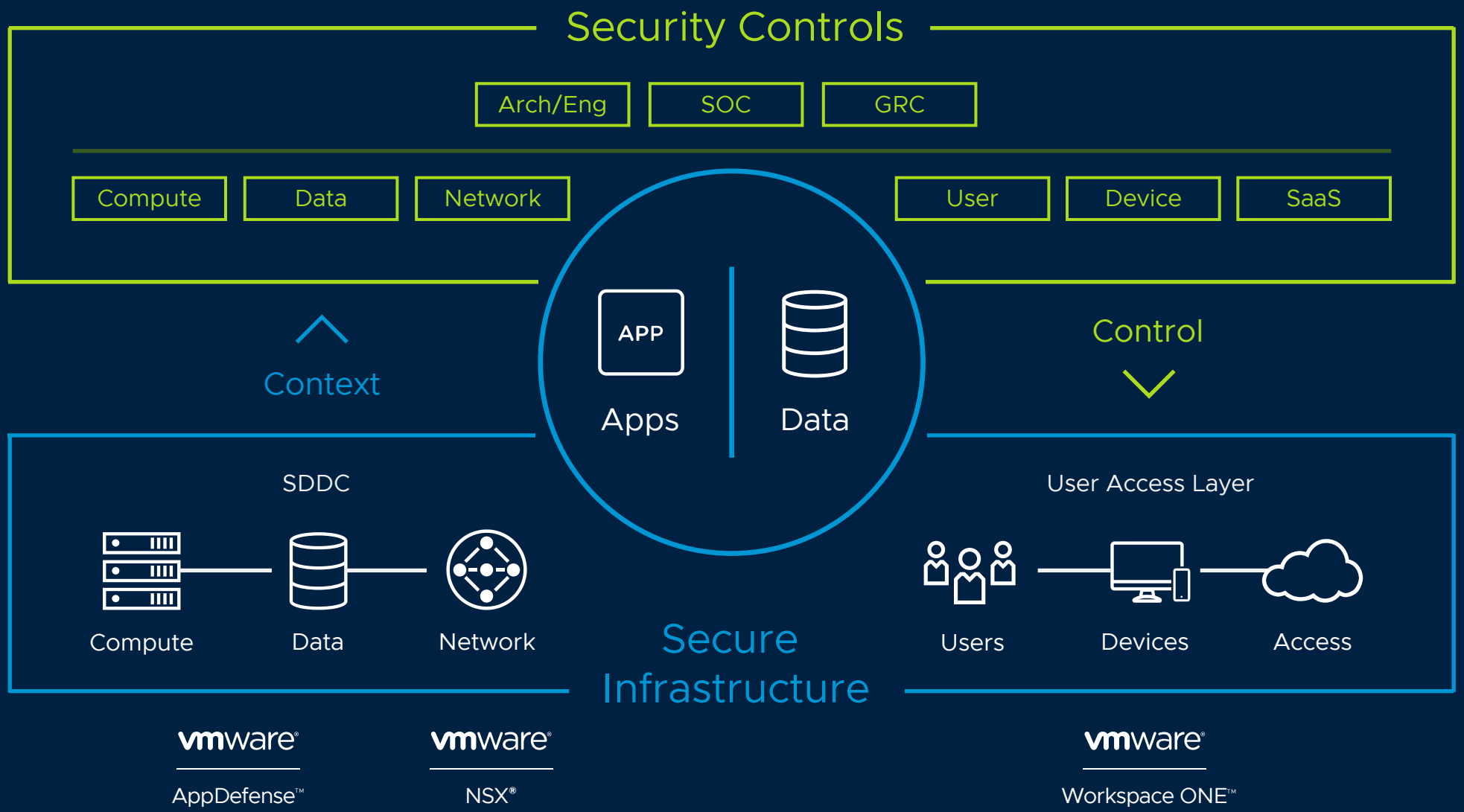
Patching

Cyber Hygiene
Attack Surface



Can the unique properties of cloud and mobile be the solution versus the problem?

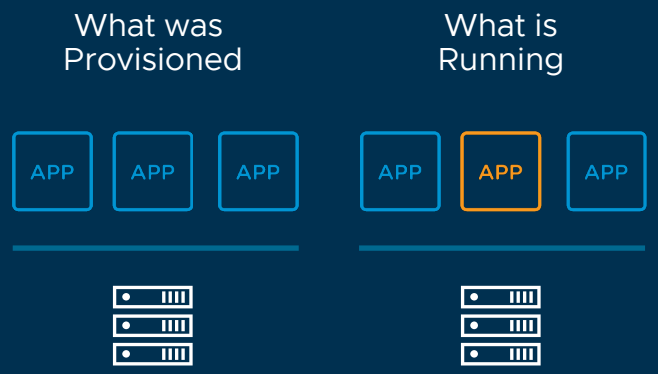




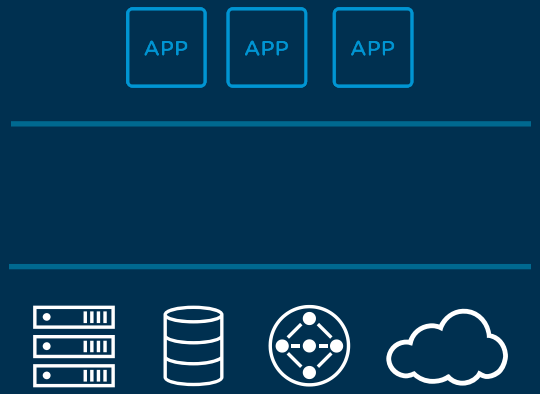
Distributed Systems Require Distributed Control Points

We Can Uniquely Leverage the Hypervisor

Application

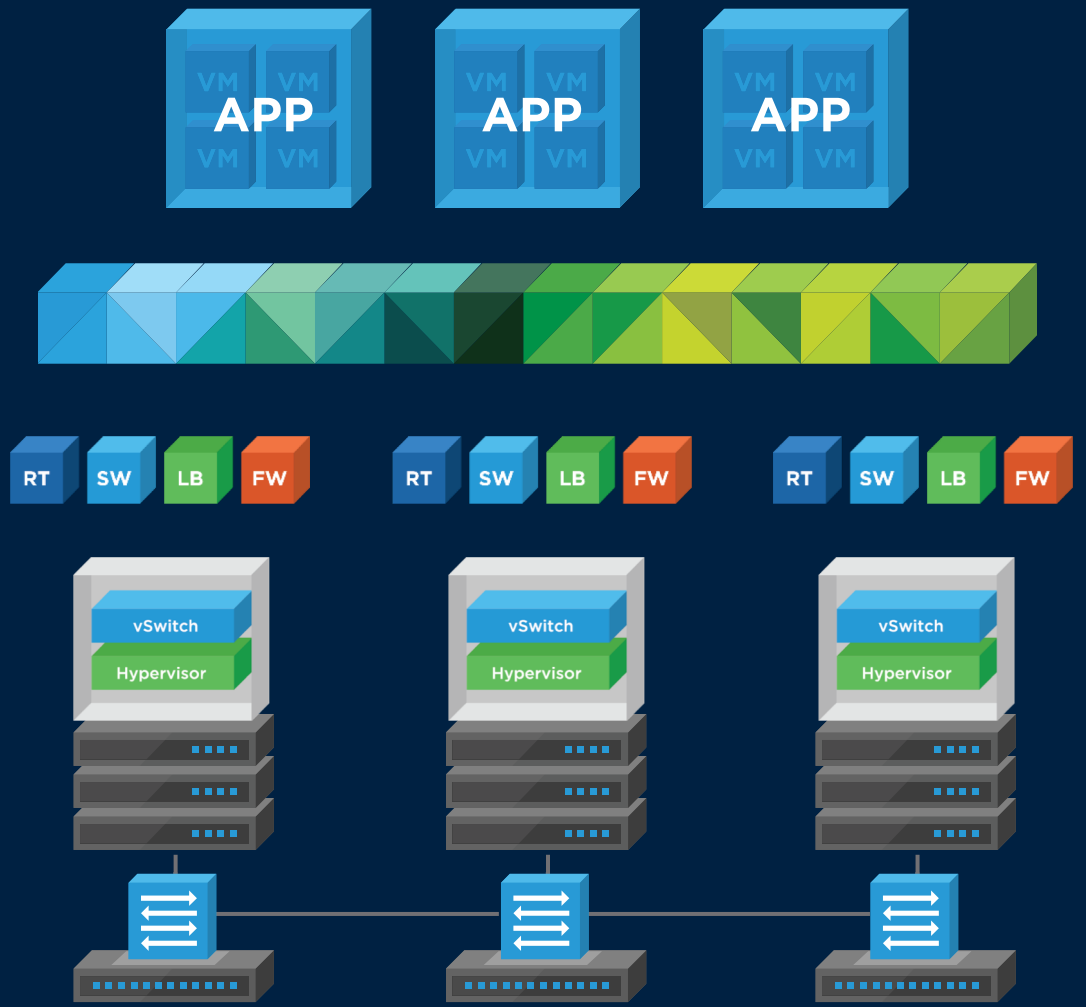


Isolation



Automation

Leveraging Hypervisor Isolation as a Control Point

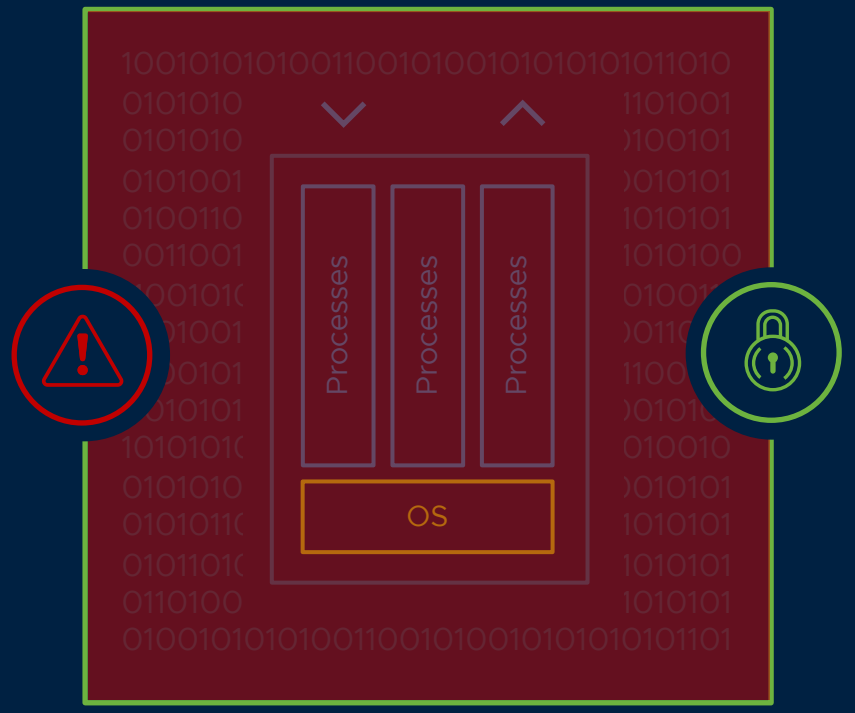


Changing the Data Center Security Model

From chasing bad to ensuring good

Chasing Bad

75,000,000



Ensuring Good

200

What You Need to Deal with at the Application Layer

You need to protect against different threat models

You are dealing with an erosion of our security anchor points (endpoint/network)

You need to operate at devops speed

vmware

Protecting Applications in Virtualized and Cloud Environments

Learn

Capture & Analyze

vm Manifest

Protect

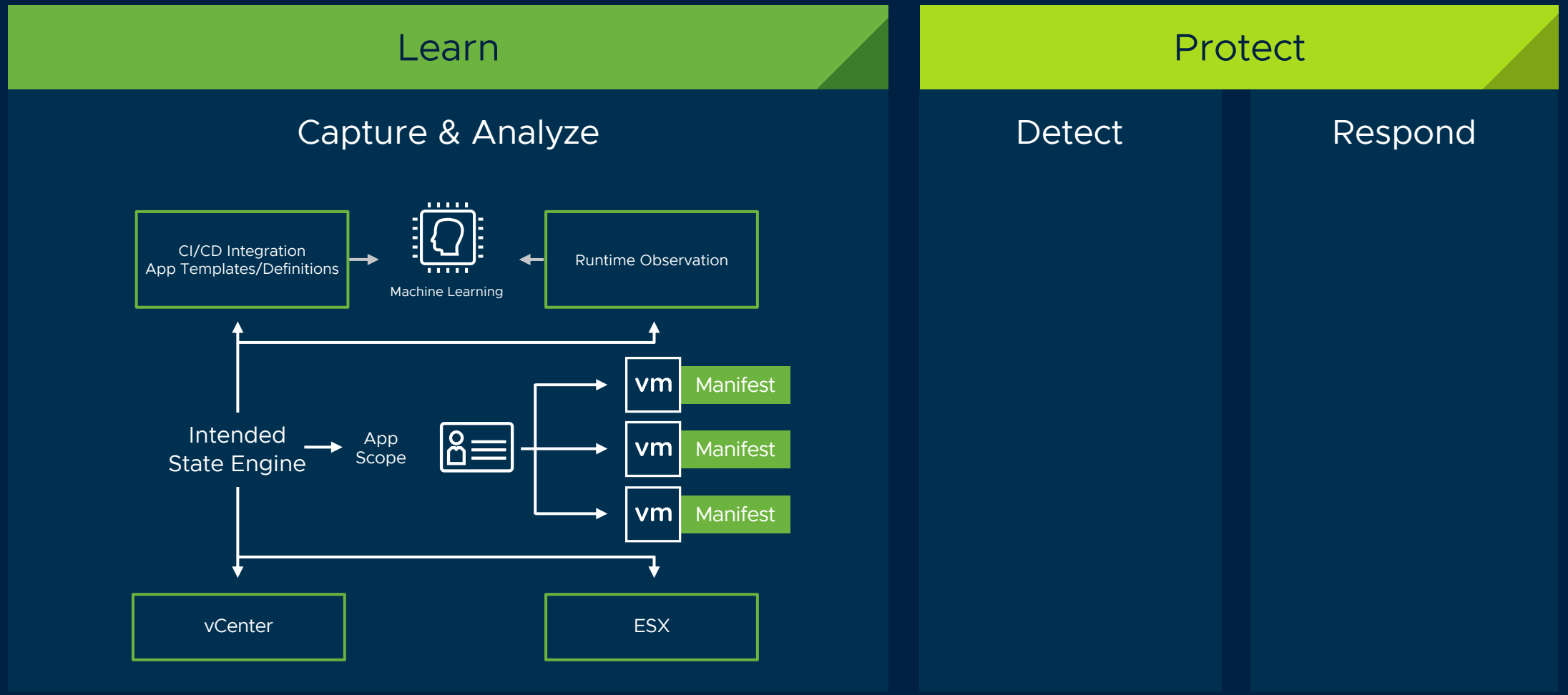
Detect

vm Manifest

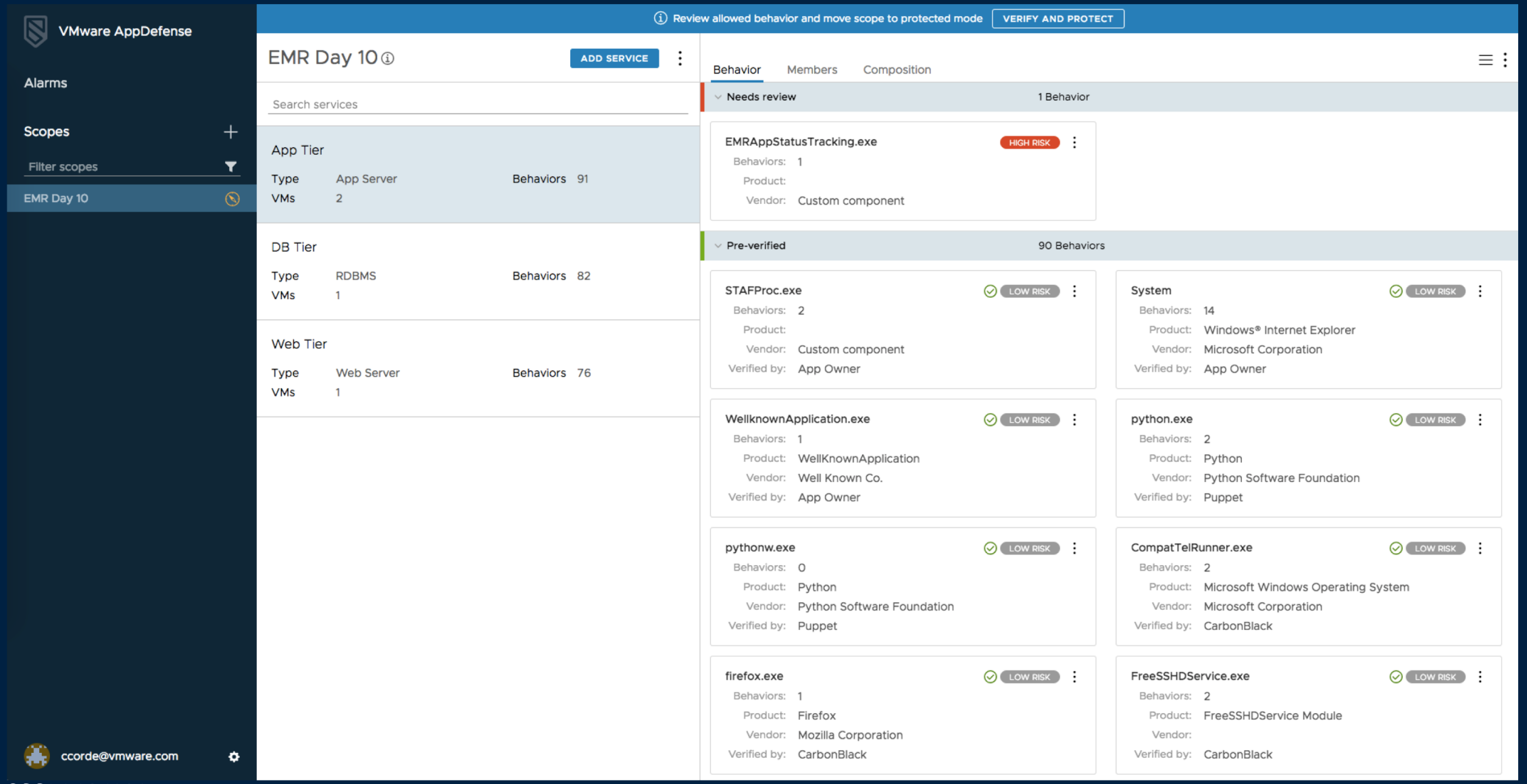
Respond

Capture & Analyze

Capture the purpose and intended state of applications and VMs

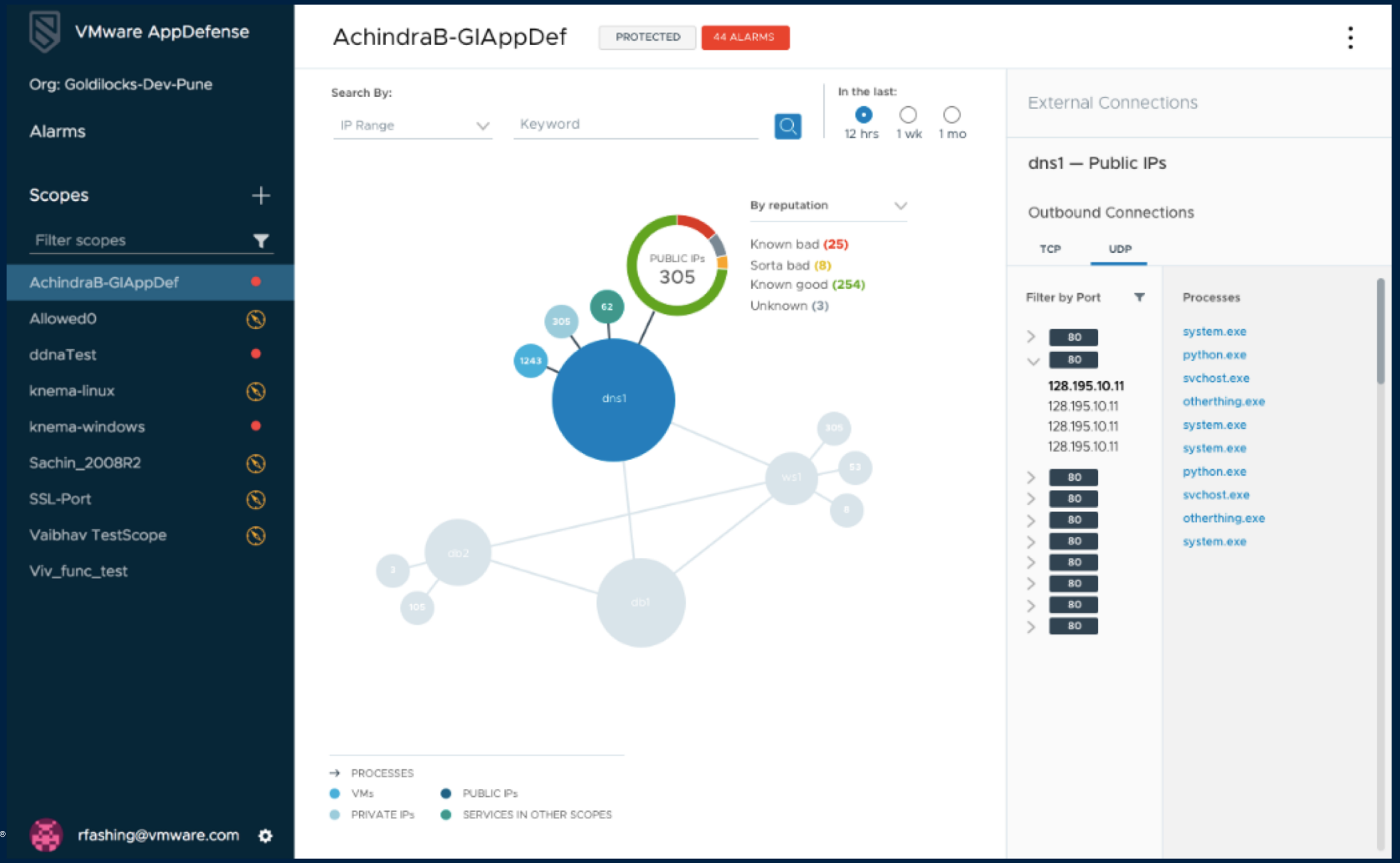


The Result - The App Manifest



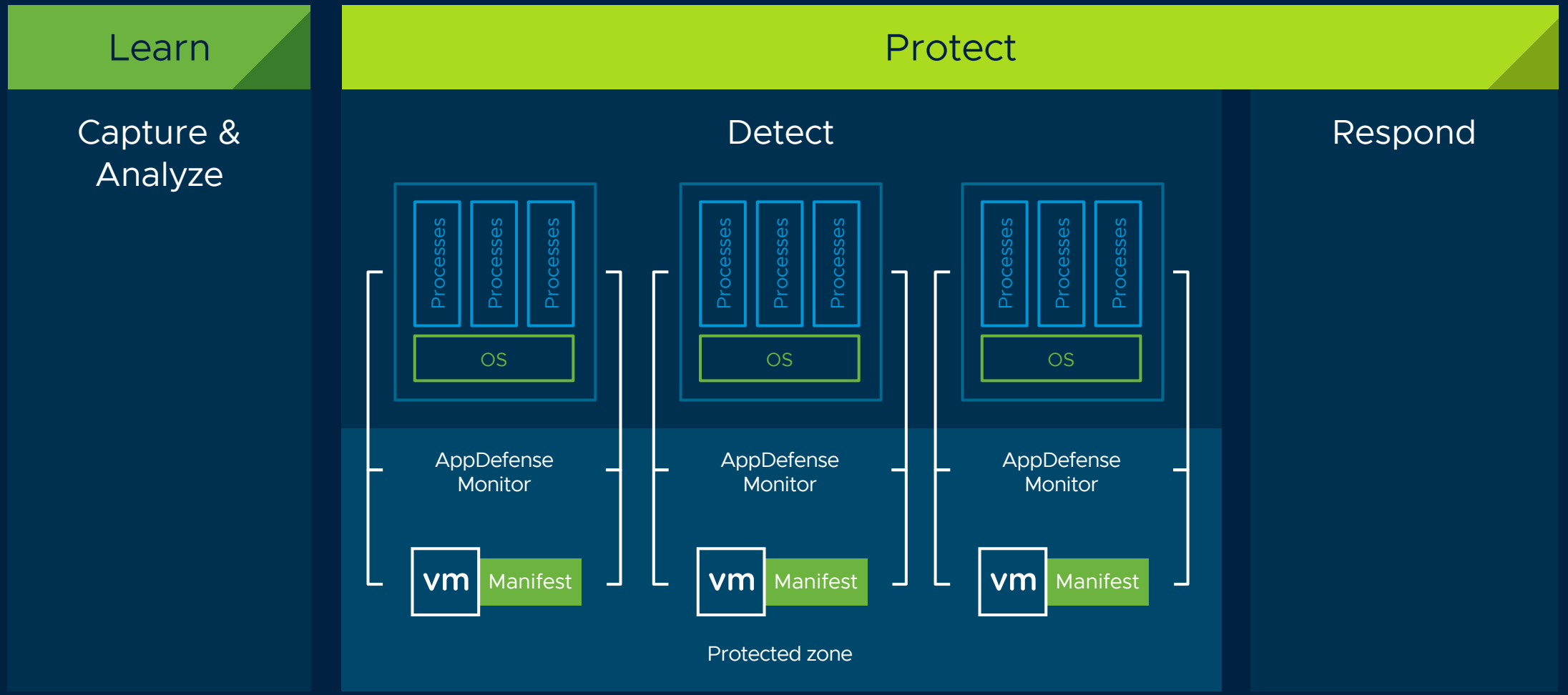
vmware

The Result – The App Manifest



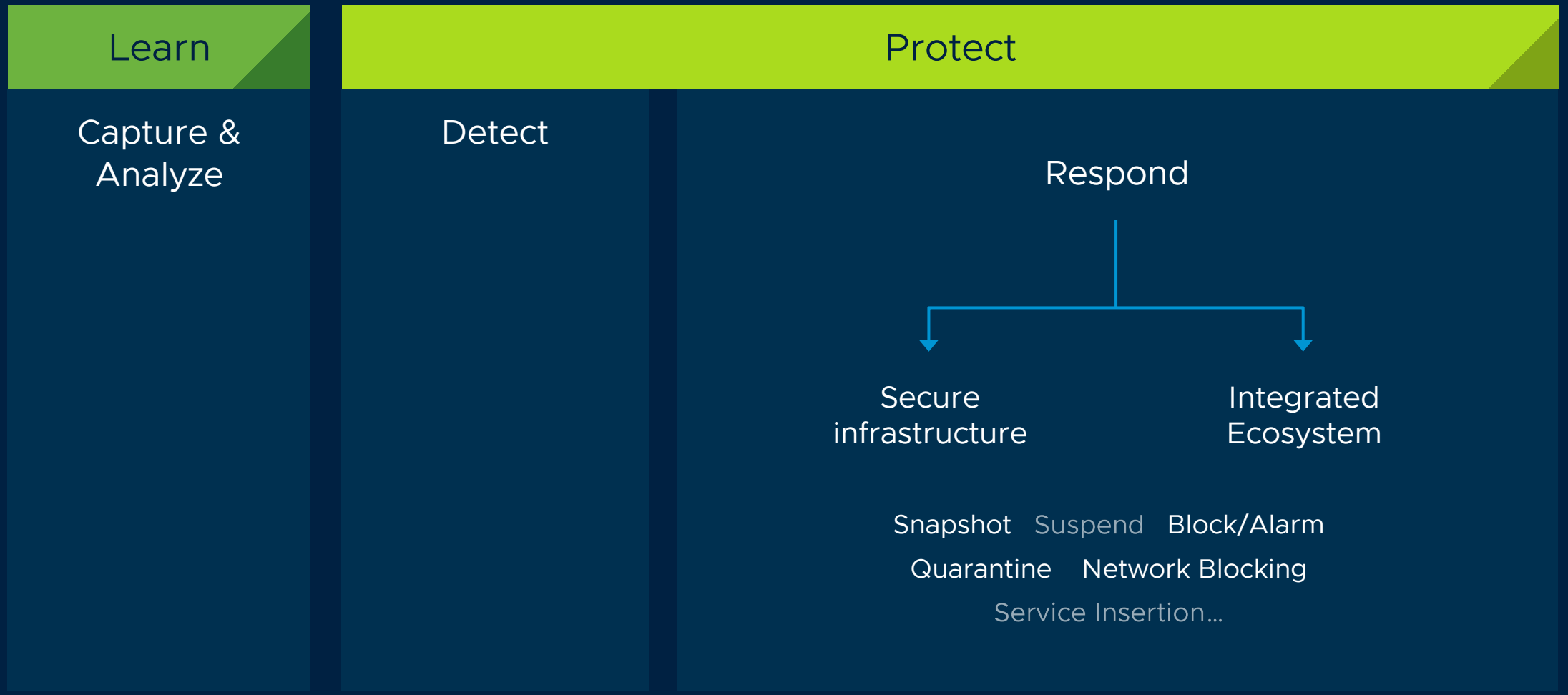
Detect

Runtime application attestation and secure manifest store



Respond

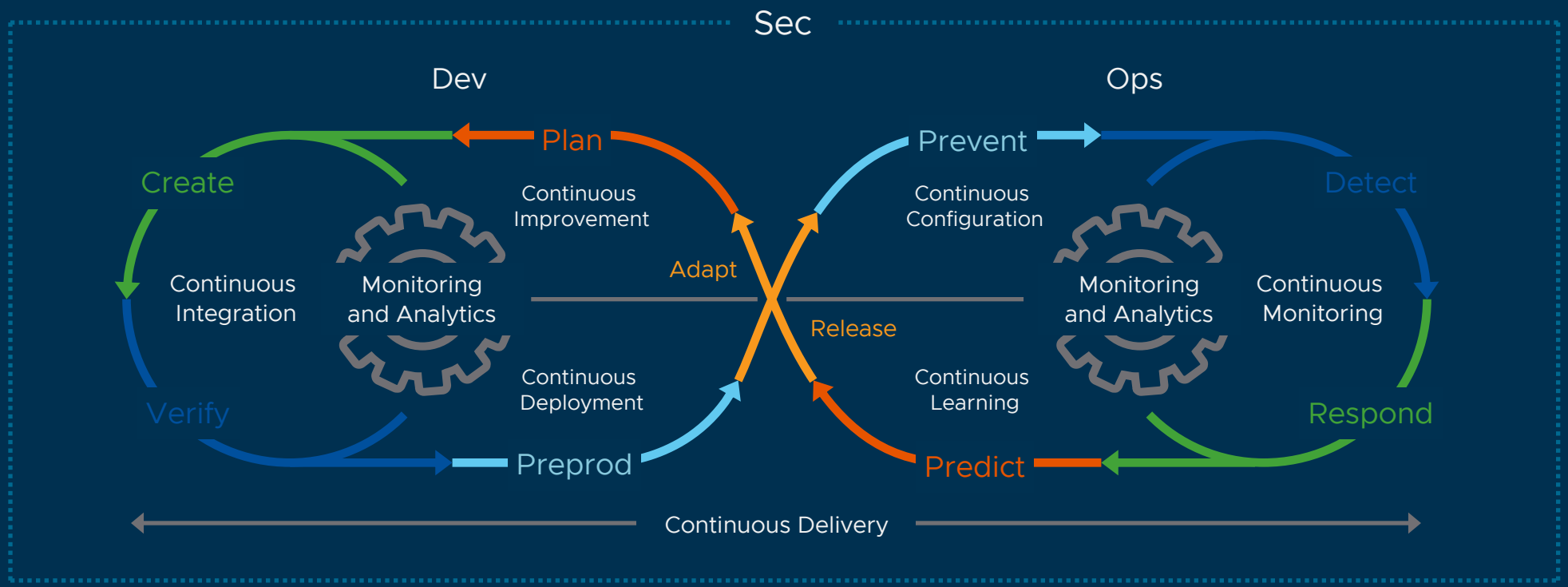
Orchestrated incident response routines for the SOC



Review and Readiness

Collaboration Between Security Teams and Application Teams

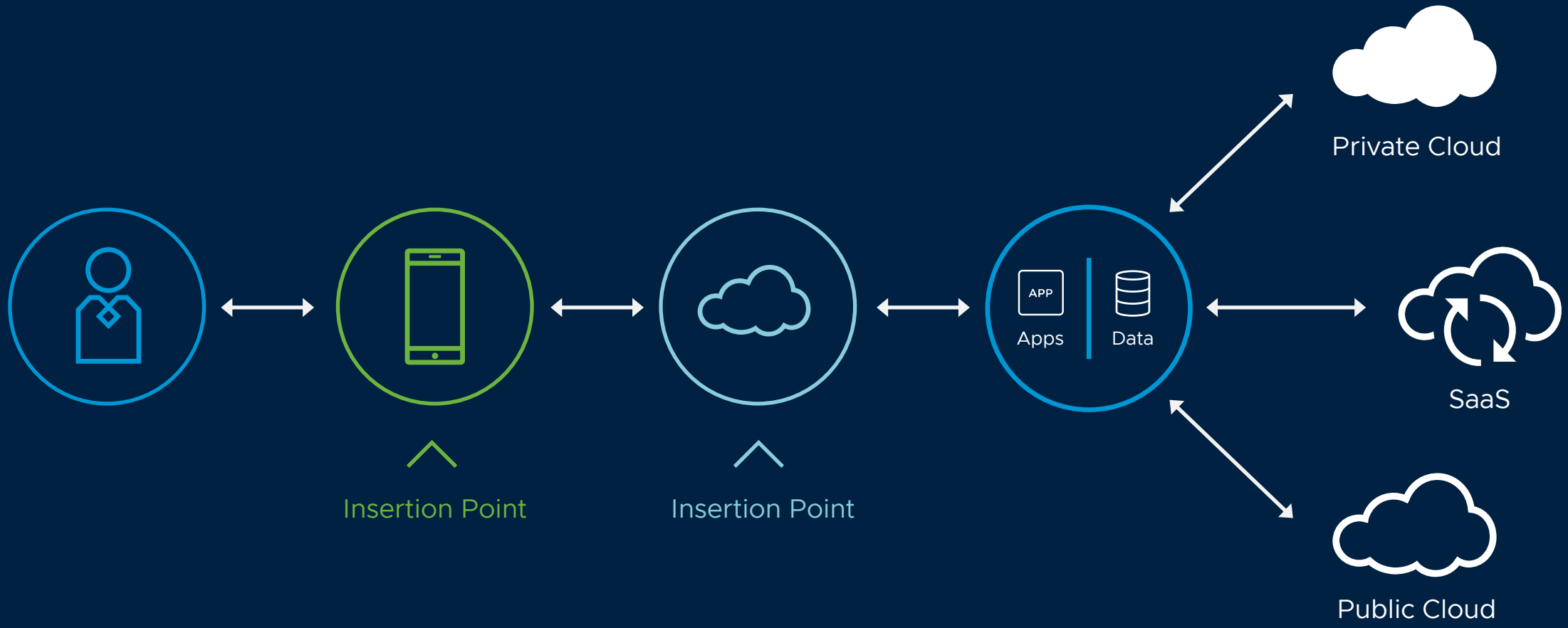
Figure 2: DevSecOps: Secure Development as a Continuous Improvement Process © 2017 Gartner, Inc.



Source: Gartner,10 Things to Get Right for Successful DevSecOps, Neil MacDonald, October 03 2017. *Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document.*

Validate and Verify

Right user + right device + right app



Security “Agility” in the view of VMware

- Use the hypervisor as a distributed & isolated boundary
- Integrate in the CI/CD pipeline to ingest application intended state and deviations
- Use the cloud to validate behavior and binaries across a larger population using consensus and to spot anomalies
- Align network and segmentation controls with process behavior knowledge in an automation fashion

Reducing the Clutter

Source: Momentum Partners Cyberscape 2017

Go beyond: Securing Cloud & Mobility

To using: Cloud & Mobility to Secure

Thanks

vmware®